

REMARKS

Claims 1-26 are pending in the current application. In an Office Action dated June 1, 2005 ("Office Action"), the Examiner requested that copies of non-patent literature previously filed with the U.S.P.T.O. on a CD-ROM be again furnished in the current response, rejected claims 1-2, 11, and 26 under 35 U.S.C. § 102(e) as being anticipated by McNabb et al., U.S. Patent No. 6,289,462 ("McNabb"), rejected claims 3-6 and 18-21 under 35 U.S.C. § 103(a) as being unpatentable over McNabb, and rejected claims 7-10, 12-17, and 22-25 under 35 U.S.C. § 103(a) as being unpatentable over McNabb in view of Quach et al., U.S. Patent No. 6, 654, 909 ("Quach"). Applicants' representative has included the requested non-patent literature in the current response, and notes that, since the non-patent literature was previously submitted on CD-ROM with the Information Disclosure Statement filed October 25, 2001, no additional fees should be due for the resubmission of this material. Applicants' representative respectfully traverses the 35 U.S.C. § 102 and 35 U.S.C. § 103 rejections, below.

The current application is directed to a new computer architecture that employs features included on new processor implementations, including the Intel IA-64, or Itanium, processors, to provide a secure platform kernel ("SPK") and secure platform global services ("SPGS") that run in a first and second privilege class above processor hardware and that, in turn, provide a virtual-machine-like interface to one or more operating systems. In other words, the current application is directed to a new computer architecture in which one or more operating systems run above a virtual-machine-like interface provided by a secure platform that includes an SPK and an SPGS layer that are both more privileged than the operating systems that run above them. In this new architecture, unlike in current computer architectures, operating systems cannot directly execute privileged instructions, and hardware resources protected by privileges more privileged than the privilege level at which the operating systems execute cannot be accessed by the one or more operating systems that run above the virtual-machine interface. This new architecture is discussed, in overview, beginning on line 11 of page 4 in the current application.

Claim 1 of the current application is next provided, for the Examiner's convenience:

1. A computer system comprising:
  - at least one processor;
  - a memory;
  - a secure platform stored in the memory for controlling the processor and the memory;
  - an operating system image stored in the memory for controlling the processor and the memory and operating on top of the secure platform;
  - an end user application stored in the memory for controlling the processor and the memory and operating on top of the operating system image; and
  - wherein the secure platform is configured to provide a secure partition within the memory for storing secret data associated with and accessible by the end user application, the secure partition being inaccessible to the operating system and other tasks operating on top of the secure platform.

Claim 1 claims a computer system including a processor, memory, a secure platform, an operating system that operates on top of the secure platform and that is distinct from the operating system, and an end-user application that operates on top of the operating system. Thus, claim 1 reflects the above-discussed, new computer architecture to which the current application is directed. Moreover, claim 1 specifically claims that the secure platform provides a secure partition within memory of the computer system for storing secret data associated with, and accessible by, the end-user application, but inaccessible to the operating system. In currently available computer architectures, there is no computer resource that cannot be accessed by the operating system. By contrast, in the new computer architecture towards which the current application is directed, the operating system cannot access certain resources of the computer system, including privileged instructions and memory associated with privilege levels more highly privileged than the privilege level at which the operating system executes. Independent claims 12, 18, and 26 also recite the secure platform and the fact that the secure platform provides memory accessible to application programs but inaccessible to operating systems within the new type of computer system to which the current application is directed.

McNabb is completely unrelated to the claimed subject matter of the current application. McNabb describes what McNabb characterizes as a new security layer within a currently available operating system, namely the Unix operating system. The new security level comprises, as explicitly stated by McNabb, beginning on line 11 of column 7, operating system security enhancements, network packet management modifications, upgrade/downgrade enforcer, security gate, trusted administration utilities, enhanced secure shell, authentication module, secure CGI module, network layer encryption, and usage of the Secure Socket Layer encryption. In other words, McNabb has enhanced a currently available operating system, and employs various operating-system-level and higher-level features and utilities in order to produce the trusted server system to which McNabb's patent is directed. McNabb again explicitly states the fact that McNabb's disclosed trusted server system merely represents various operating-system-level and higher-level enhancements to a standard computer system, beginning on line 57 of column 8 and continuing through line 8 of column 9:

The key components discussed below for the trusted operating system are as follows: 1) processes; 2) file system objects (including devices, directories, files, etc.); and 3) interprocess communication messages (including packets, shared memory, etc.). On a standard system, each of these has various security attributes, which are created, managed, and used by the OS itself. When a process attempts to access a file system object, the OS compares various attributes of the process with attributes of the object, and allows or denies access. When a process sends or receives communication messages, the OS verifies that the process is allowed to send and/or receive the message. When objects are created, such as when a file is created or when a message is generated, the OS is responsible for ensuring that the proper attributes are attached to the new object.

The trusted server system has extended this standard mechanism in two ways: by attaching additional security attributes to each of the OS components, and by extending the security checks to use the new attributes. (emphasis added)

In other words, McNabb neither teaches, mentions, nor suggests a new computer architecture with a secure platform executing at a higher privilege level than an operating system, but simply discloses an enhanced operating system. This fact is explicitly stated in McNabb in many additional places, including, beginning on line 60 of column 10:

In the preferred embodiment of the Unix implementation, the trusted server system comprises a computer executing the kernel process of the present invention where in addition to the default inode structure information, a link is included to retrieve previously stored attribute label information related to the file.

In rejecting claim 1, the Examiner cites column 7, lines 11-20 of McNabb as teaching the secure-platform element of claim 1. As discussed above, the cited portion of McNabb teaches nothing of the sort. Instead, the cited portion of McNabb teaches that McNabb's trusted server system comprises merely a number of operating-system security enhancements, and employment of various other operating-system-level or higher-level features and utilities. Furthermore, the Examiner cites lines 20-24 of column 4 as teaching, in part, provision of a secure partition by a secure platform for storing secret data associated with, and accessible by, an end-user application but inaccessible to the operating system. The cited portion of column 4 merely states that a goal of McNabb's trusted server system is to provide "a secure platform for network services, where users can install the system and immediately begin taking advantage of its security features. . ." The fact that McNabb uses the phrase "secure platform" to stand for an entirely different concept than that for which the phrase "secure platform" stands in the current application is irrelevant. Furthermore, there is no mention in the cited portion of column 4 of memory accessible both to the secure platform and an end-user application, but not to an operating system.

The Examiner further cites lines 7-17 and 52-61 of column 17 as teaching provision of a secure partition accessible to an end-user application but not to an operating system. The first of the cited passages of column 17 discusses a web server used to display static web pages and to provide connectivity to back-end applications. A web server is not part of a virtual-machine-like interface provided by a secure platform that includes an SPK and SPGS that both run at privilege levels more privileged than an operating system. Moreover, this cited portion of column 17 does not teach, mention, or suggest data accessible to applications and a secure platform but not accessible to an operating system. The second cited passage of column 17 is directed to attributes assigned to processes, files, and other resources that partition programs, data, and

network interfaces to isolate programs, data, and network interfaces from each other and from an externally accessible compartment that is accessible by the general public. However, this passage explicitly states that this ability to partition a network server is a key component of the "trusted operating system of the present invention." In other words, the passage again explicitly states that the operating system may access any of these partitions since it is the operating system that partitions the programs, data, and network interfaces. There is no mention in this passage, or anywhere else in McNabb, of an SPK or SPGS that together compose a secure platform running at greater privilege level than an operating system and managing system resources that are inaccessible to an operating system. McNabb is completely unrelated to the current application.

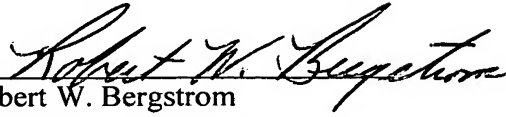
Quach explicitly states that Quach's patent is related "to the design of highly reliable microprocessors and more specifically to the use of a dedicated state machine that periodically checks the validity of critical processor resources" (Quach, Abstract). In other words, Quach discloses a feature of a processor architecture, and the error-detection state machine disclosed by Quach is explicitly shown, in Figure 1, as a component of a processor. The current application is not directed to processor architectures. Quach is completely unrelated to the current application.

Neither McNabb, Quach, nor McNabb and Quach in combination teach, mention, or suggest a secure platform distinct from an operating system, such as the currently disclosed and claimed SPK and SPGS, that runs at a privilege level higher than the privilege level at which one or more operating systems. Neither McNabb nor Quach teach, mention, or suggest a memory partition that is accessible by an end-user application and a secure platform, but not accessible to an operating system. As discussed above, McNabb discloses operating system enhancements, and Quach discloses a state-machine included in a processor implementation. For this reason, McNabb is completely unsuitable to an anticipatory reference for a 35 U.S.C. § 102 rejection of any of the current claims, McNabb is unsuitable for a 35 U.S.C. § 103 rejection of any of the current claims, and McNabb and Quach in combination are unsuitable for a 35 U.S.C. §

103 rejection of any of the current claims.

The application is now clearly in order for allowance.

Respectfully submitted,  
Robert W. Gardner  
Olympic Patent Works PLLC

  
Robert W. Bergstrom  
Registration No. 39,906

Enclosures:

Postcard

Transmittal in duplicate

Olympic Patent Works PLLC  
P.O. Box 4277  
Seattle, WA 98194-0277  
206.621.1933 telephone  
206.621.5302 fax